

In the Claims:

Please amend Claims 1, 21, 40, 49, 50 and 60, cancel Claims 20, 39 and 62-65 and add new Claims 66-70, all as shown below. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer implemented method for modifying a list of permitted senders used by electronic mail (email) access control devices, said method comprising:

under control of a sender:

accepting a recipient identifier;

providing sender information along with a petition provider identifier to a recipient, the recipient having an access list of permitted senders associated therewith;

under control of the recipient:

providing the sender information to a petition provider identified by the petition provider identifier;

accepting an access list petition request (petition) from the petition provider, said petition being stored in a computer readable storage medium;

determining whether the petition is acceptable based on at least one of: 1) a sender identity verification method; 2) user input; and 3) third party information; and

modifying said access list of permitted senders of the recipient such that the sender is added to said access list if the petition is determined to be acceptable; and

wherein the petition is ~~received and evaluated at a time~~ created as a result of the sender ~~receives~~ receiving the recipient's email address and prior to transmission of email messages between said sender and said recipient; and

wherein the access list is used to determine whether email from the sender is permitted to reach the recipient. ~~petition is transmitted through a different protocol than said email messages in order to avoid said petition from being filtered.~~

2. (Previously Presented) The method of claim 1 wherein:
the sender information includes at least one of: 1) a sender identification method; and 2) the recipient identifier.
3. (Original) The method of claim 1, further comprising:
providing confirmation of the determination to the sender.
4. (Original) The method of claim 1 wherein:
the step of accepting the recipient identifier is a result of a Web-based interaction between the recipient and the sender.
5. (Original) The method of claim 1 wherein:
the recipient identifier is an email address.
6. (Original) The method of claim 1 wherein:
the identity verification method is one of: 1) an email header "From" address; 2) a password; 3) an Internet Protocol (IP) address; and 4) a digital signature.
7. (Original) The method of claim 1 wherein:
the step of determining whether a petition is acceptable utilizes at least one rule, wherein the at least one rule is evaluated against the petition.
8. (Original) The method of claim 1, further comprising:
prompting a user for a decision regarding whether or not to accept the petition.
9. (Original) The method of claim 1 wherein:
the recipient comprises a Web browser.

10. (Original) The method of claim 9 wherein:

the sender information is provided to the petition provider via a Hypertext Transfer Protocol (HTTP) redirect sent to the Web browser.

11. (Original) The method of claim 9 wherein:

the petition is provided to a petition processor via a Hypertext Transfer Protocol (HTTP) redirect message sent to the Web browser; and

wherein the petition processor makes said determination.

12. (Previously Presented) The method of claim 9 wherein:

the Web browser identifies the petition based on a Multipurpose Internet Mail Extension (MIME) type.

13. (Previously Presented) The method of claim 9 wherein:

the petition provider identifier and the sender information are combined to form a Uniform Resource Locator (URL) that the Web browser uses to access the petition provider.

14. (Original) The method of claim 1, further comprising:

providing the petition to a petition processor.

15. (Original) The method of claim 14 wherein:

the petition processor requires authorization credentials.

16. (Previously Presented) The method of claim 1 wherein:

the sender identity verification method is used by an email provider to verify that an email message is from the sender.

17. (Original) The method of claim 1 wherein:

the petition provider generates the petition based on one or more rules.

18. (Previously Presented) The method of claim 17 wherein:

a rule determines at least one of: 1) whether to generate the petition; 2) a format of the petition; 3) an identity of a petition processor; and 4) a recipient email address.

19. (Previously Presented) The method of claim 17 wherein:

a rule is triggered based on the recipient identifier.

20. (Canceled)

21. (Currently Amended) A computer implemented method for modifying a list of permitted senders used by electronic mail (email) access control devices, said method comprising:

under control of a sender:

accepting a recipient identifier;

generating an access list petition request (petition) wherein said generation is based on the evaluation of at least one rule that determines the format of the petition based on the recipient identifier, said petition being stored in a computer readable medium;

providing the petition to a recipient, the recipient having an access list of permitted senders associated therewith;

under control of the recipient:

accepting the petition;

determining whether the petition is acceptable based on at least one of: 1) a sender identity verification method; 2) user input; and 3) third party information; and

modifying said access list of permitted senders of the recipient such that the sender is added to said access list if the petition is determined to be acceptable;

wherein the petition is ~~received and evaluated at a time~~ created as a result of the sender receives receiving the recipient's email address and prior to transmission of email messages between said sender and said recipient; and

wherein the access list is used to determine whether email from the sender is permitted to reach the recipient.

22. (Original) The method of claim 21, further comprising:

providing the recipient identifier to a petition provider; and

accepting a petition from the petition provider.

23. (Previously Presented) The method of claim 21 wherein:

the sender information includes at least one of: 1) a sender identification method; and 2) the recipient identifier.

24. (Original) The method of claim 22 wherein:

the petition provider and the sender are part of the same system.

25. (Original) The method of claim 21 wherein:

the step of accepting the recipient identifier is a result of a Web-based interaction between the recipient and the sender.

26. (Original) The method of claim 21 wherein:

the recipient identifier is an email address.

27. (Original) The method of claim 21 wherein:

the identity verification method is one of: 1) an email header "From" address; 2) a password; 3) an Internet Protocol (IP) address; and 4) a digital signature.

28. (Original) The method of claim 21 wherein:

the step of determining whether a petition is acceptable utilizes at least one rule, wherein the at least one rule is evaluated against the petition.

29. (Original) The method of claim 21, further comprising:
prompting a user for a decision regarding whether or not to accept the petition.
30. (Original) The method of claim 21 wherein:
the recipient comprises a Web browser.
31. (Original) The method of claim 30 wherein:
the petition is provided to a petition processor via a Hypertext Transfer Protocol (HTTP) redirect sent to the Web browser; and
wherein the petition processor makes said determination.
32. (Previously Presented) The method of claim 30 wherein:
the Web browser identifies the petition based on a Multipurpose Internet Mail Extension (MIME) type.
33. (Original) The method of claim 21, further comprising:
providing the petition to a petition processor.
34. (Original) The method of claim 33 wherein:
the petition processor requires authorization credentials.
35. (Previously Presented) The method of claim 21 wherein:
the sender identity verification method is used by a petition processor to verify that an email message is from the sender.
36. (Original) The method of claim 22 wherein:
the petition provider generates the petition based on one or more rules.

37. (Previously Presented) The method of claim 36 wherein:

a rule determines at least one of: 1) whether to generate the petition; 2) a format of the petition; 3) an identity of a petition processor; 4) a recipient email address.

38. (Previously Presented) The method of claim 36 wherein:

a rule is triggered based on the recipient identifier.

39. (Canceled)

40. (Currently Amended) A computer implemented method for modifying a list of permitted senders used by electronic mail (email) access control devices, said method comprising:

providing a recipient email address to the sender;

providing a petition to the recipient, wherein the petition includes a sender identity verification method;

determining whether the petition is acceptable based on authorization credentials and at least one of: 1) the sender identity verification method; 2) user input; and 3) third party information;

modifying an email access list of permitted senders by adding the sender to said email access list if the petition and the authorization credentials are acceptable;

wherein the petition is ~~received and evaluated at a time~~ created as a result of the sender receives receiving said recipient email address ~~and prior to transmission of email messages between said sender and said recipient; and~~

~~wherein the petition is transmitted by using a different protocol than said email messages in order to avoid said petition from being filtered; and~~

wherein the email access list is used to determine whether or not email from the sender is permitted to reach the recipient.

41. (Original) The method of claim 40, further comprising:

providing confirmation of the determination to the sender.

42. (Original) The method of claim 40 wherein:

the step of providing the recipient email address to the sender is a result of a Web-based interaction between the recipient and the sender.

43. (Previously Presented) The method of claim 40 wherein:

the sender identity verification method is used by the recipient to verify that an email message is from the sender.

44. (Original) The method of claim 40 wherein:

the identity verification method is one of: 1) an email header "From" address; 2) a password; 3) an Internet Protocol (IP) address; and 4) a digital signature.

45. (Original) The method of claim 40 wherein:

the petition is provided to a Web browser.

46. (Previously Presented) The method of claim 45 wherein:

the Web browser identifies the petition based on a Multipurpose Internet Mail Extension (MIME) type.

47. (Original) The method of claim 40 wherein:

the step of determining whether a petition is acceptable utilizes at least one rule, wherein the at least one rule is evaluated against the petition.

48. (Original) The method of claim 40, further comprising:

prompting a user for a decision regarding whether or not to accept the petition.

49. (Currently Amended) A system comprising:

a means for providing a recipient email address to the sender;

a means for providing a petition to the recipient, wherein the petition includes a sender identity verification method;

a means for determining whether the petition is acceptable based on authorization credentials and at least one of: 1) the sender identity verification method; 2) user input; and 3) third party information;

a means for modifying an email access list of permitted senders by adding the sender to said email access list if the petition and the authorization credentials are acceptable;

wherein the petition is ~~received and evaluated at a time~~ created as a result of the sender ~~receives~~ receiving said recipient email address ~~and prior to transmission of email messages between said sender and said recipient; and~~

~~wherein the petition is transmitted by using a different protocol than said email messages in order to avoid said petition from being filtered; and~~

wherein the email access list is used to determine whether or not email from the sender is permitted to reach the recipient.

50. (Currently Amended) A system for modifying a list of permitted senders used by electronic mail (email) access control devices, said method comprising:

a sender component operable to accept a recipient identifier and generate sender information, wherein the sender information can be used to generate a petition;

a petition provider component operable to generate a petition based on the sender information and at least one rule, said petition being stored in a computer readable medium; and

wherein the petition is generated ~~at a time~~ as a result of the sender component ~~receives~~ receiving said recipient identifier ~~and prior to transmission of email messages between said sender component and a recipient; and~~

~~wherein the petition is transmitted by using a different protocol than said email messages in order to avoid said petition from being filtered; and~~

wherein the petition includes a sender identity verification method which ~~can be~~ is used to verify the identity of the sender.

51. (Original) The system of claim 50, further comprising:

a web browser operable to accept the sender information from the sender component and provide the sender information to the petition provider component.

52. (Original) The system of claim 50, further comprising:

a petition processor component operable to accept the petition and determine whether the petition is acceptable based on at least one of: 1) the sender identity verification method; 2) user input; and 3) third party information; and

wherein if the petition is acceptable, the sender component is permitted to send email to a recipient associated with the recipient identifier.

53. (Original) The system of claim 52, further comprising:

a web browser operable to accept the petition from the petition provider component and to provide the petition to the petition processor.

54. (Previously Presented) The system of claim 52 wherein:

the petition processor component provides a confirmation to the sender.

55. (Previously Presented) The system of claim 52 wherein:

the browser identifies the petition based on a Multipurpose Internet Mail Extension (MIME) type.

56. (Original) The system of claim 50 wherein:

the sender identification verification method is one of: 1) an email header "From" address; 2) a password; 3) an Internet Protocol (IP) address; and 4) a digital signature.

57. (Original) The system of claim 52 wherein:

the petition processor determines whether or not to accept a petition and add the sender to an email access list for a recipient.

58. (Previously Presented) The method of claim 50 wherein:

the at least one rule determines at least one of: 1) whether to generate the petition; 2) a format of the petition; and 3) an identity of a petition processor.

59. (Previously Presented) The method of claim 50 wherein:

the at least one rule is triggered based on the recipient identifier.

60. (Currently Amended) A machine readable medium having instructions stored thereon that when executed by a processor cause a system to:

accept a recipient identifier;

provide a petition to a recipient wherein the recipient corresponds to the recipient identifier and wherein the petition is based on the evaluation of at least one rule, said recipient having an access list of permitted senders associated therewith;

determine whether the petition is acceptable based on at least one of: 1) a sender identity verification method; 2) user input; and 3) third party information; and

modifying said access list of permitted senders of the recipient such that a sender associated with said petition is added to the access list if the petition is determined to be acceptable;

wherein the petition is ~~provided to the recipient at the time~~ created as a result of accepting the recipient identifier and ~~prior to transmission of email messages between the sender and the recipient;~~

~~wherein the petition is provided by using a different protocol from said email messages;~~
and

wherein if the request petition is acceptable, the sender is permitted by the access list to send email to the recipient.

61-65. (Canceled)

66. (New) The method of claim 1 wherein modifying the access list adds the sender to at least one of: a white list of senders permitted to send email to the recipient and a black list of senders prohibited from sending email to the recipient.

67. (New) The method of claim 1, further comprising:

communicating, from the recipient to the sender, a confirmation of the outcome of the petition that specifies whether the sender was added to the access list of the recipient.

68. (New) A computer readable storage medium having instructions stored thereon, which instructions when executed by one or more processors, cause a system to:

under control of a sender:

accept a recipient identifier;

provide sender information along with a petition provider identifier to a recipient, the recipient having an access list of permitted senders associated therewith;

under control of the recipient:

provide the sender information to a petition provider identified by the petition provider identifier;

accept an access list petition request (petition) from the petition provider, said petition being stored in a computer readable storage medium;

determine whether the petition is acceptable based on at least one of: 1) a sender identity verification method; 2) user input; and 3) third party information; and

modify said access list of permitted senders of the recipient such that the sender is added to said access list if the petition is determined to be acceptable; and

wherein the petition is created as a result of the sender ~~receives~~ receiving the recipient's email address; and

wherein the access list is used to determine whether email from the sender is permitted to reach the recipient.

69. (New) The computer readable storage medium of claim 68 wherein modifying the access list adds the sender to at least one of: a white list of senders permitted to send email to the recipient and a black list of senders prohibited from sending email to the recipient.

70. (New) The computer readable storage medium of claim 68, further comprising instructions that cause the system to:

communicate, from the recipient to the sender, a confirmation of the outcome of the petition that specifies whether the sender was added to the access list of the recipient.